Aix-Marseille Université
Institut Universitaire de Technologie
Département Réseaux et Télécommunications

Année 2020-2021
M1204
Numération et calculs

Algèbre fondamentale

Table des matières

1 Quelques rappels sur les nombres réels

1.1 L'ensemble $\mathbb{N}$

C'est l'ensemble des entiers naturels (c'est-à-dire des nombres entiers supérieurs ou égaux à 0) :

$$\boxed{\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}}$$

Quel que soit n appartenant à $\mathbb{N}$, $n+1$ appartient également à $\mathbb{N}$, ce qui, avec des quantificateurs, s'écrit aussi :

$$\forall n,\ (n \in \mathbb{N}) \Rightarrow (n+1 \in \mathbb{N}).$$

De plus, toute partie A de $\mathbb{N}$ contenant 0, et qui est stable par l'application $n \to n+1$, c'est-à-dire qui satisfait la condition

$$\forall n \in \mathbb{N},\ (n \in A) \Rightarrow (n+1 \in A),$$

est forcément égale à $\mathbb{N}$: $A = \mathbb{N}$.
Cette propriété est à la base du raisonnement par récurrence.

1.1.1 Principe du raisonnement par récurrence

Soit $P(n)$ un énoncé dépendant de l'indice n (qui est un entier naturel) tel que :
- *$P(0)$ est vrai*
- *pour tout entier naturel n fixé, on a l'implication ($P(n)$ est vrai) $\Rightarrow$ ($P(n+1)$ est vrai).*

Alors, en vertu du principe de raisonnement par récurrence, l'énoncé $P(n)$ est vrai pour tout $n \in \mathbb{N}$.

Exercice. Pour tout réel $a \neq 1$, montrer par récurrence sur l'entier n que :

$$\boxed{\underbrace{1 + a + a^2 + \ldots + a^n}_{\sum_{p=0}^{n} a^p} = \frac{1 - a^{n+1}}{1 - a}}$$

1.1.2 Dénombrement

Soient E un ensemble fini à n éléments, $E = \{x_1, x_2, \ldots, x_n\}$ et p un entier de $\{1, 2, \ldots, n\}$.

p-arrangements sans répétition de n éléments. *On appelle p-arrangements sans répétition de n éléments de E toute liste ordonnée du type*

$$(x_{i_1}, x_{i_2}, \ldots, x_{i_p}),$$

où les indices $i_1, i_2, \ldots, i_p$ sont deux à deux distincts (ce qui implique que les éléments d'une telle liste sont également deux à deux distincts). Ainsi, deux p-arrangements diffèrent :
- *soit par la nature de leurs éléments*
- *soit par l'ordre dans lequel sont rangés ces éléments.*

On note A_n^p le nombre (cardinal) de tous ces p-arrangements sans répétition de n éléments. On a donc :

$$A_n^p = A_n^{p-1} \times [n - (p-1)].$$

D'où, successivement :

$$\left\{\begin{array}{ccc} A_n^{p-1} & = & A_n^{p-2} \times [n-(p-2)] \\ A_n^{p-2} & = & A_n^{p-3} \times [n-(p-3)] \\ \vdots & \vdots & \vdots \\ A_n^2 & = & A_n^1 \times (n-1) \\ A_n^1 & = & n \end{array}\right.$$

En multipliant membre à membre ces égalités, on obtient finalement :

$$\boxed{A_n^p = n(n-1)(n-2)\ldots(n-p+1)}$$

Si l'on introduit la notation $n!$, qui se lit $factorielle\ n$, où

$$n! = n \times (n-1) \times (n-2) \times \ldots \times 3 \times 2 \times 1,$$

avec la convention $0! = 1$, l'égalité précédente s'écrit simplement :

$$\boxed{A_n^p = \frac{n!}{(n-p)!}}$$

$Cas\ particulier.$ Si $p = n$, A_n^p désigne alors le nombre de $permutations\ (des\ n\ éléments)\ de\ E$. D'après la formule précédente, le nombre de permutations de E est :

$$\boxed{p_n = n!}$$

Combinaisons de n éléments pris p à p. *Toute sous partie F de E contenant p éléments, $F = \{x_{i_1}, x_{i_2}, \ldots, x_{i_p}\}$, dans laquelle ces éléments sont distincts et énoncés dans un ordre quelconque, est appelée $combinaison\ de\ n\ éléments\ pris\ p\ à\ p$. On note C_n^p leur nombre.*
Les éléments de chacune de ces combinaisons pouvant être ordonnés de $p!$ façons différentes, on a donc

$$p!C_n^p = A_n^p,$$

ce qui implique :

$$\boxed{C_n^p = \frac{n!}{p!(n-p)!}}$$

Lorsque $p = 0$, il n'y a qu'un seul sous-ensemble de E ne contenant aucun élément (c'est l'ensemble vide). C'est pourquoi on convient de poser :

$$\boxed{C_n^0 = 1}$$

$Propriétés\ des\ C_n^p$. Les propriétés essentielles à retenir sont les suivantes :

$$\boxed{\begin{array}{ll} (i) & C_n^p \in \mathbb{N} \\ (ii) & C_n^p = C_n^{n-p} \\ (iii) & C_n^p = C_{n-1}^p + C_{n-1}^{p-1} \quad \textit{(formule de Pascal)} \end{array}}$$

La formule de Pascal est à la base du $triangle\ de\ Pascal$:

C_n^p	p=0	p=1	p=2	p=3	p= 4	p=5	p= 6	p=7	p=8	p= 9
n=0	1									
n=1	1	1								
n=2	1	2	1							
n=3	1	3	3	1						
n=4	1	4	6	4	1					
n=5	1	5	10	10	5	1				
n=6	1	6	15	20	15	6	1			
n=7	1	7	21	35	35	21	7	1		
n=8	1	8	28	56	70	56	28	8	1	
n=9	1	9	36	84	126	126	84	36	9	1

Une application importante : la formule du binôme de Newton. *Quels que soient les réels a et b, quel que soit $n \in \mathbb{N}^*$, on démontre (par récurrence sur n) la formule suivante (à connaître) :*

$$\boxed{(a+b)^n = \underbrace{a^n + C_n^1 a^{n-1} b + C_n^2 a^{n-2} b^2 + \ldots + C_n^{n-1} a b^{n-1} + b^n}_{\displaystyle\sum_{p=0}^{n} C_n^p a^{n-p} b^p}}$$

Exemples. Quels que soient $a \in \mathbb{R}$ *et* $b \in \mathbb{R}$*, la formule du binôme appliquée successivement pour* $n = 2, 3, 4, 5, 6, 7, 8$ *et* 9 *donne :*

$$\begin{array}{rcl}
(a+b)^2 & = & a^2 + 2ab + b^2 \\
(a+b)^3 & = & a^3 + 3a^2b + 3ab^3 + b^3 \\
(a+b)^4 & = & a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \\
(a+b)^5 & = & a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5 \\
(a+b)^6 & = & a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6 \\
(a+b)^7 & = & a^7 + 7a^6b + 21a^5b^2 + 35a^4b^3 + 35a^3b^4 + 21a^2b^5 + 7ab^6 + b^7 \\
(a+b)^8 & = & a^8 + 8a^7b + 28a^6b^2 + 56a^5b^3 + 70a^4b^4 + 56a^3b^5 + 28a^2b^6 + 8ab^7 + b^8 \\
(a+b)^9 & = & a^9 + 9a^8b + 36a^7b^2 + 84a^6b^3 + 126a^5b^4 + 126a^4b^5 + 84a^3b^6 + 36a^2b^7 + 9ab^8 + b^9.
\end{array}$$

1.2 L'ensemble $\mathbb{R}$

C'est l'ensemble des nombres réels qui contient (strictement) celui des nombres rationnels (noté $\mathbb{Q}$*) :*

$$\boxed{\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}}$$

L'ensemble $\mathbb{R}$ *est muni d'une addition et d'une multiplication (ce sont des lois de composition interne). Elles satisfont notamment :*

$$\begin{array}{cc}
(i) & (a + c = b + c) \Rightarrow (a = b) \\
(ii) & (ac = bc \text{ et } c \neq 0) \Rightarrow (a = b)
\end{array}$$

L'implication (a) *s'énonce en disant que* $\textit{tout élément de } \mathbb{R} \textit{ est régulier pour l'addition.}$ *Quant à* (b)*, elle exprime que* $\textit{tout élément non nul de } \mathbb{R} \textit{ est régulier pour la multiplication.}$
D'autre part, il résulte de (ii) *que :*

$$(ab = 0) \Rightarrow (a = 0 \text{ ou } b = 0)$$

1.2.1 Propriétés liées à la relation d'ordre

L'ensemble $\mathbb{R}$ *est totalement ordonné par la relation* $\leq$*. Cette relation est* $\textit{compatible avec l'addition}$ *:*

$$\forall a, b, c \in \mathbb{R}, \ (a \leq b) \Rightarrow (a + c \leq b + c),$$

et $\textit{compatible avec la multiplication par un réel positif}$ *:*

$$\forall a, b \in \mathbb{R}, \ \forall c \in \mathbb{R}^+, \ (a \leq b) \Rightarrow (ac \leq bc).$$

Remarque. Attention de bien vérifier que $c \geq 0$ *avant d'utiliser cette dernière implication.*

1.2.2 Valeur absolue

Pour tout $x \in \mathbb{R}$*, on appelle* $\textit{valeur absolue de } x$*, le réel positif noté* $|x|$*, qui est défini par*

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x \leq 0. \end{cases}$$

On vérifie alors que $|x| = \max(x, -x)$*, et l'on a les propriétés suivantes :*

$$\boxed{\begin{array}{cl}
(i) & |x| \in \mathbb{R}_+ \text{ et } (|x| = 0) \Leftrightarrow (x = 0) \\
(ii) & |xy| = |x||y| \\
(iii) & ||x| - |y|| \leq |x + y| \leq |x| + |y|
\end{array}}$$

Exercice. Vérifier que l'on a $\max(x, y) = \frac{1}{2}(x + y + |x - y|)$ *et* $\min(x, y) = \frac{1}{2}(x + y - |x - y|)$ *pour tout* $x \in \mathbb{R}$ *et* $y \in \mathbb{R}$*.*

1.2.3 Partie entière

Soit x un réel. On appelle $\textit{partie entière de } x$*, le plus grand entier relatif inférieur ou égal à x :*

$$E(x) = \max\{n \in \mathbb{Z},\ n \leq x\}$$

Il résulte directement de cette définition que $E(x)$ est l'unique entier relatif satisfaisant la double inégalité suivante :

$$\boxed{E(x) \leq x < E(x) + 1}$$

Exemples. $E(3.7) = 3$, $E(-2) = -2$, $E(-2.4) = -3$ *et* $E(-5.718) = -6$.

1.2.4 Puissances et radicaux

Il est facile de définir les puissances entières d'un réel x :

$$\begin{cases} x^0 = 1 \\ \forall n \in \mathbb{N},\ x^{n+1} = x^n \times x \\ \forall n \in \mathbb{N},\ x^{-n} = \frac{1}{x^n} \quad (x \neq 0). \end{cases}$$

Dans la suite du cours de $1^{\text{ère}}$ année, on verra que l'application $x \mapsto x^n$ $(n \in \mathbb{N}^*)$ est une bijection de $\mathbb{R}^+$ sur lui-même, dont l'application réciproque permet de définir la $\textit{racine } n^{\text{ième}}$*, notée $\sqrt[n]{}$, et définie par l'équivalence :*

$$\begin{cases} \sqrt[n]{x} = y \\ y \in \mathbb{R}_+ \end{cases} \Leftrightarrow \begin{cases} x = y^n \\ x \in \mathbb{R}_+. \end{cases}$$

En clair, cela signifie que la racine $n^{\text{ième}}$ du réel positif x est l'unique réel positif y satisfaisant $x = y^n$. Pour tout $x \geq 0$, on note également $\sqrt[n]{x} = x^{\frac{1}{n}}$ et plus généralement, si $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$:

$$x^{\frac{p}{q}} = \sqrt[q]{x^p}.$$

Les principales propriétés des exposants rationnels (à savoir) sont les suivantes :

$$\boxed{\forall x \in \mathbb{R}_+,\ \forall r, s \in \mathbb{Q},\ \begin{cases} x^r x^s & = & x^{r+s} \\ (x^r)^s & = & x^{rs} \end{cases}}$$

et

$$\boxed{\forall x, y \in \mathbb{R}_+,\ \forall r \in \mathbb{Q},\ (xy)^r = x^r y^r}$$

2 Nombres complexes

Il est bien connu que l'équation $x^2+1=0$ *n'a pas de solution dans* $\mathbb{R}$.
L'objectif de ce chapitre est de construire un nouvel ensemble de nombres, noté $\mathbb{C}$, *et nommé* $ensemble\ des\ nombres\ complexes$, *qui soit tel que :*

— $\mathbb{R} \subset \mathbb{C}$
— *l'addition et la multiplication définies sur* $\mathbb{R}$ *s'étendent à* $\mathbb{C}$
— *toute équation du second degré possède au moins une solution dans* $\mathbb{C}$.

2.1 Généralités

2.1.1 Construction de $\mathbb{C}$

On rappelle que l'égalité de deux couples de réels est définie par

$$((a,b)=(a',b')) \Longleftrightarrow \left(\begin{array}{c} a=a' \\ b=b' \end{array}\right).$$

On va définir sur l'ensemble de ces couples de réels, $\mathbb{R}^2$, $\mathbb{R}^2=\{(a,b),\ a\in\mathbb{R} \text{ et } \mathrm{b}\in\mathbb{R}\}$, *une addition et une multiplication qui "prolongent" l'addition et la multiplication dans* $\mathbb{R}$. *L'ensemble* $\mathbb{R}^2$ *muni de ces deux opérations sera* $\mathbb{C}$.

Addition et multiplication par un réel. *Soient* $z=(a,b)$ *et* $z'=(a',b')$ *où* a, a', b *et* b' *sont des réels et soit* λ *un réel. Par définition, on pose :*

$$\left\{\begin{array}{rcl} z+z' & = & (a+a',b+b') \\ \lambda z & = & (\lambda a,\lambda b). \end{array}\right.$$

On voit ainsi que

$$z=(a,b)=a(1,0)+b(0,1) \tag{1}$$

Le <u>*réel*</u> a *s'appelle alors* $partie\ réelle\ de\ z$, *ce que l'on note* $\mathrm{Re}\,(z)=a$, *et le* <u>*réel*</u> b *s'appelle* $partie\ imaginaire\ de\ z$, *ce que l'on note* $\mathrm{Im}\,(z)=b$.
Si $b=0$ *alors* $z=a(1,0)$: z *est dit* $réel$ *et l'on note plus simplement* $z=a$.
Si $a=0$ *alors* $z=b(0,1)$: z *est dit* $imaginaire\ pur$. *En posant ensuite*

$$i=(0,1),$$

on obtient tout simplement $z=bi$, *ce qu'il est également d'usage de noter* $z=ib$.
Toutes ces conventions permettent finalement de définir $l'écriture\ algébrique$ *de n'importe quel nombre complexe* z,

$$z=(a,b)=a+ib \text{ avec a} \in \mathbb{R} \text{ et b} \in \mathbb{R}$$

qui est équivalente à (1).

Produit de deux nombres complexes. *Soient* $z=(a,b)$ *et* $z'=(a',b')$. *Par définition on pose*

$$z\times z'=(aa'-bb',ab'+a'b)=zz'.$$

On vérifie alors que $(0,1)^2=(-1,0)$, *c'est-à-dire avec les notations qui viennent d'être introduites :*

$$\boxed{i^2=-1}$$

De plus :

— $\underbrace{(1,0)}_{1}\times\underbrace{(a,b)}_{z}=(a,b)\times(1,0)=(a,b)$ *donc* $1\times z=z\times 1=z$, *ce qui montre que* $1=(1,0)$ *est élément neutre de la multiplication dans* $\mathbb{C}$.
— *pour tout* $z=(a,b)\neq(0,0)$, *le complexe* $z'=\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)$ *vérifie* $zz'=z'z=1$. *Tout complexe non nul* z *possède un inverse* z' *noté* $\frac{1}{z}$.

On dit que $\mathbb{C}$ *(muni des opérations d'addition et de multiplication ainsi définies) est un* $corps$. *Les calculs dans* $\mathbb{C}$ *obéissent aux lois habituelles de l'algèbre en tenant compte de l'égalité* $i^2=-1$.

Conjugaison. *Pour tout $z = (a,b)$, on appelle* conjugué de z *le nombre complexe $\overline{z} = a - ib = (a,-b)$. On remarque alors immédiatement que*

$$\boxed{\mathrm{Re}\,(z) = \frac{z+\overline{z}}{2} \qquad \mathrm{Im}\,(z) = \frac{z-\overline{z}}{2i}}.$$

Conséquence. On obtient directement les deux équivalences suivantes :

$$\left\{\begin{array}{ccccc} (i) & z \text{ est réel} & \iff & z = \overline{z} \\ (ii) & z \text{ est imaginaire pur} & \iff & z = -\overline{z} \end{array}\right.$$

On vérifie ensuite facilement pour tous complexes z et z', que :

$$\boxed{\begin{array}{ccc} \overline{z+z'} & = & \overline{z}+\overline{z'} \\ \overline{zz'} & = & \overline{z}\,\overline{z'} \\ \overline{\lambda\, z} & = & \lambda\,\overline{z},\ \lambda \in \mathbb{R} \end{array}}$$

Retour sur la résolution de l'équation du second degré $ax^2+bx+c=0$, $(a,b,c) \in \mathbb{R}^* \times \mathbb{R}^2$. *Comme $a \neq 0$, on peut écrire*

$$ax^2+bx+c=0 \iff a\left[\left(x+\frac{b}{2a}\right)^2 - \frac{1}{4a^2}\underbrace{(b^2-4ac)}_{\Delta}\right] = 0.$$

Ainsi, pour chaque $\delta \in \mathbb{C}$ tel que $\delta^2 = \Delta$, on aura :

$$\begin{aligned} \left(ax^2+bx+c=0\right) &\iff \left(\left[x+\frac{b}{2a}\right]^2 - \frac{\delta^2}{4a^2} = 0\right) \\ &\iff \left(\left[x-\frac{-b+\delta}{2a}\right]\left[x-\frac{-b-\delta}{2a}\right] = 0\right) \\ &\iff \left(x = \frac{-b\pm\delta}{2a}\right) = x_\pm. \end{aligned}$$

Maintenant, si

- *$\Delta > 0$, $\delta = \pm\sqrt{\Delta} \in \mathbb{R}$, et $x_\pm = \frac{-b\pm\sqrt{\Delta}}{2a}$ sont deux racines réelles distinctes.*
- *$\Delta = 0$, $\delta = 0$, donc $x_+ = x_- = \frac{-b}{2a}$ est l'unique racine réelle.*
- *$\Delta < 0$, $\delta = \pm i\sqrt{-\Delta} \in i\mathbb{R}$, donc $x_\pm = \frac{-b\pm i\sqrt{-\Delta}}{2a}$ sont deux racines complexes conjuguées.*

2.1.2 Représentation géométrique d'un nombre complexe

L'analogie de l'écriture $z = a(1,0)+b(0,1)$ avec l'écriture vectorielle $\overrightarrow{OM} = a\vec{u}+b\vec{v}$ suggère d'associer au nombre complexe $z=(a,b)$ le point $M(a,b)$ du plan rapporté au repère orthonormé $(0,\vec{u},\vec{v})$. On dit alors que M est l'image *de z, ou que z est* l'affixe *de M.*

Remarque.

- *Si $z \in \mathbb{R}$ (z est réel) alors $M \in (Ox)$. Par contre, si $z \in i\mathbb{R}$ (z est imaginaire pur), on a $M \in (Oy)$.*
- *Le conjugué $\overline{z}$ de z a pour image le symétrique de M par rapport à (Ox).*

Image de $z+z'$. *Soient $z = a+ib$ et $z' = a'+ib'$ deux nombres complexes d'images respectives M et M'. D'après ce que l'on vient de voir, l'image de $z'' = z+z' = a+a'+i(b+b')$ est le point M'' défini par l'égalité vectorielle $\overrightarrow{OM''} = \overrightarrow{OM}+\overrightarrow{OM'}$. On a donc l'équivalence*

$$(z'' = z+z') \iff \left(\overrightarrow{OM''} = \overrightarrow{OM}+\overrightarrow{OM'}\right).$$

En particulier, si $z' = -z$, il découle de l'équivalence précédente que $\overrightarrow{OM'} = -\overrightarrow{OM}$.

Conséquence. Soient A et B deux points du plan d'affixes respectives z_A et z_B. Comme

$$\overrightarrow{AB} = \overrightarrow{AO} + \overrightarrow{OB} = \overrightarrow{OB} - \overrightarrow{OA},$$

l'unique point C tel que $\overrightarrow{OC} = \overrightarrow{AB}$ a pour affixe $z_C = z_B - z_A$. Ceci nous amène donc à associer le nombre complexe $z_B - z_A$ au vecteur $\overrightarrow{AB}$.

Application. Trouver l'expression de l'affixe z_C en fonction de z_A et z_B de sorte que $(0ABC)$ soit un parallélogramme.

Image de λz, $\lambda \in \mathbb{R}$. *Si $z = a + ib$ on sait que $z' = \lambda z = \lambda a + i(\lambda b)$. L'image de z' est donc le point M' défini par $\overrightarrow{0M'} = \lambda \overrightarrow{0M}$, soit :*

$$(z' = \lambda z) \Longleftrightarrow \left(\overrightarrow{OM'} = \lambda \overrightarrow{OM}\right).$$

2.2 Module et argument d'un nombre complexe

2.2.1 Représentation trigonométrique d'un nombre complexe

Soit M l'image de $z = a + ib$. Par définition, le $module\ de\ z$ est le nombre réel (positif)

$$\boxed{|z| = \|\overrightarrow{OM}\| = \sqrt{a^2 + b^2}}$$

et, lorsque $z \neq 0$, on appelle $Argument\ de\ z$ (avec un "A" majuscule), toute mesure en radians (définie à 2π-près) de l'angle $(\widehat{\vec{u}, \overrightarrow{OM}})$:

$$\boxed{\text{Arg } z = \text{mes}(\widehat{\vec{u}, \overrightarrow{OM}})}$$

Remarque.

- *$|z| \geq 0$ pour tout $z \in \mathbb{C}$.*
- *Le nombre complexe 0 n'a pas d'argument.*
- *Lorsque $z \neq 0$, Arg z est défini à 2π-près : il existe un unique réel $\theta \in [0, 2\pi[$ tel que*

$$\text{Arg } z = \theta + 2k\pi,\ k \in \mathbb{Z}.$$

Par commodité, pour tout $z \neq 0$, on appellera $argument\ de\ z$ (avec un "a" minuscule) cette valeur de θ (appartenant à $[0, 2\pi[$) :

$$\boxed{\arg z = \theta}$$

En résumé, pour tout complexe z non nul, on l'équivalence suivante :

$$\left(\begin{array}{c} a = r\cos\theta \\ b = r\sin\theta \end{array}\right) \Longleftrightarrow \left(\begin{array}{c} r = \sqrt{a^2 + b^2} \\ \cos\theta = \frac{a}{r} \quad \sin\theta = \frac{b}{r} \end{array}\right),$$

ce qui fournit l'$écriture\ trigonométrique$ de z :

$$\boxed{z = r(\cos\theta + i\sin\theta) \text{ avec } r \in \mathbb{R}^+ \text{ et } \theta \in \mathbb{R}.}$$

Remarque. Lorsque $a \neq 0$, on a $\tan\theta = \frac{b}{a}$. Cependant, cette égalité ne détermine θ qu'à π-près (puisque $\tan(\theta + \pi) = \tan\theta$). Pour déterminer θ, on doit choisir l'angle θ pour lequel $\cos\theta$ a bien le signe de a. En résumé :

$$\left(\begin{array}{c} a = r\cos\theta \\ b = r\sin\theta \end{array}\right) \Longleftrightarrow \left(\begin{array}{c} r = \sqrt{a^2 + b^2} \\ \tan\theta = \frac{b}{a} \quad \text{sgn }(a) = \text{sgn }(\cos\theta) \end{array}\right).$$

2.2.2 Module et argument du produit

Soient $z = r(\cos\theta + i\sin\theta)$ *et* $z' = r'(\cos\theta' + i\sin\theta')$ *deux nombres complexes. Par un calcul simple, on obtient*

$$zz' = rr'\left[\underbrace{(\cos\theta\cos\theta' - \sin\theta\sin\theta')}_{\cos(\theta+\theta')} + i\underbrace{(\sin\theta\cos\theta' + \cos\theta\sin\theta')}_{\sin(\theta+\theta')}\right],$$

ce qui entraîne :

$$\boxed{\begin{cases} |zz'| & = & |z| \times |z'| \\ \mathit{Arg}(zz') & = & \mathit{Arg}(z) + \mathit{Arg}(z') \end{cases}}$$

Conséquences.

— *Pour tout* $n \in \mathbb{N}$, $|z^n| = |z|^n$ *et* $\mathit{Arg}(z^n) = n\mathit{Arg}(z)$

— $\left|\frac{1}{z}\right| = \frac{1}{|z|}$ *et* $\mathit{Arg}\left(\frac{1}{z}\right) = -\mathit{Arg}(z)$.

2.3 Notation exponentielle

2.3.1 Fonction exponentielle complexe

Pour tout nombre complexe $z = a + ib$, *on pose :*

$$\boxed{\mathrm{e}^z = \mathrm{e}^a(\cos b + i\sin b)}$$

La fonction suivante, notée exp, *définie par*

$$\begin{array}{rccc} \exp : & \mathbb{C} & \to & \mathbb{C} \\ & z = a + ib & \mapsto & \mathrm{e}^z, \end{array}$$

s'appelle $\mathit{fonction\ exponentielle\ complexe}$ *car c'est une fonction (à valeurs complexes) de la variable complexe* z.

Remarque.,Avec cette définition :

— *Si* $z = a \in \mathbb{R}$, *on retrouve l'exponentielle réelle :* $\mathrm{e}^z = \mathrm{e}^a$

— *Si* $z = ib \in i\mathbb{R}$, *on obtient* $\mathrm{e}^{ib} = \cos b + i\sin b$

— $|\mathrm{e}^z| = \mathrm{e}^a$ *et* $\mathit{Arg}(\mathrm{e}^z) = b + 2k\pi$, $k \in \mathbb{Z}$. *En d'autres termes,* e^z *est le nombre complexe de module* e^a *dont un argument est* b.

2.3.2 Forme exponentielle d'un nombre complexe

Formule de Moivre. *En partant de l'écriture trigonométrique de n'importe quel nombre complexe* z, $z = r(\cos\theta + i\sin\theta)$, *il résulte immédiatemment de la définition de l'exponentielle complexe que*

$$\boxed{z = r(\cos\theta + i\sin\theta) = r\mathrm{e}^{i\theta} \text{ avec } r \in \mathbb{R}^+ \text{ et } \theta \in \mathbb{R}.}$$

On dit alors que le nombre complexe z *est mis sous* $\mathit{forme\ exponentielle}$.
On a déjà vu que si $z = \cos\theta + i\sin\theta$ *et* $z' = \cos\theta' + i\sin\theta'$ *alors* $zz' = \cos(\theta + \theta') + i\sin(\theta + \theta')$. *On déduit ainsi de la définition précédente l'égalité suivante :*

$$\boxed{\mathrm{e}^{i\theta}\mathrm{e}^{i\theta'} = \mathrm{e}^{i(\theta+\theta')}}$$

En choisissant $\theta' = \theta$, *on obtient ainsi* $(\mathrm{e}^{i\theta})^2 = \mathrm{e}^{i2\theta}$, *donc, par récurrence immédiate sur* <u>*l'entier naturel* n</u>, *on obtient :*

$$(\mathrm{e}^{i\theta})^n = \mathrm{e}^{in\theta}. \tag{2}$$

En prenant ensuite $\theta' = -\theta$ *et en remarquant que* $\mathrm{e}^{i0} = 1$, *on obtient*

$$\boxed{\mathrm{e}^{-i\theta} = \frac{1}{\mathrm{e}^{i\theta}} = \overline{\mathrm{e}^{i\theta}}},$$

donc, en appliquant la formule (2) au réel $-\theta$, il vient

$$\underbrace{(\mathrm{e}^{-i\theta})^n}_{\frac{1}{(\mathrm{e}^{i\theta})^n}} = \mathrm{e}^{-in\theta},$$

ce qui implique :

$$(\mathrm{e}^{i\theta})^{-n} = \mathrm{e}^{-in\theta} = \mathrm{e}^{i(-n)\theta}.$$

Par suite, nous avons démontré pour tout nombre réel θ et pour tout entier relatif n que

$$(\mathrm{e}^{i\theta})^n = \underbrace{\mathrm{e}^{in\theta}}_{\cos(n\theta)+i\sin(n\theta)},$$

ce qui démontre la formule de Moivre :

$$\boxed{\forall\theta\in\mathbb{R},\ \forall n\in\mathbb{Z},\ (\cos\theta+i\sin\theta)^n = \cos(n\theta)+i\sin(n\theta) \text{ i.e. } (\mathrm{e}^{i\theta})^n = \mathrm{e}^{in\theta}}$$

Application. La formule de Moivre permet d'exprimer $\cos(n\theta)$ en fonction des quantités $\cos^p\theta$ et $\sin^p\theta$ pour $0\le p\le n$ i.e. de puissances de cosinus et de sinus, comme on peut le voir sur cet exemple :

$$\begin{aligned}
\cos(3\theta) &= \operatorname{Re}\left(\mathrm{e}^{i3\theta}\right)\\
&= \operatorname{Re}\left(\cos(3\theta)+i\sin(3\theta)\right)\\
&= \operatorname{Re}\left((\cos\theta+i\sin\theta)^3\right)\\
&= \operatorname{Re}\left(\cos^3\theta+3\cos^2\theta(i\sin\theta)+3\cos\theta(i\sin\theta)^2+(i\sin\theta)^3\right)\\
&= \operatorname{Re}\left(\cos^3\theta-3\cos\theta\sin^2\theta+i(3\cos^2\theta\sin\theta-\sin^3\theta)\right)\\
&= \cos^3\theta-3\cos\theta\sin^2\theta.
\end{aligned}$$

Formules d'Euler. *En partant de la double égalité*

$$\mathrm{e}^{\pm i\theta} = \cos\theta \pm i\sin\theta,$$

on obtient facilement les formules d'Euler suivantes :

$$\boxed{\sin\theta = \frac{\mathrm{e}^{i\theta}-\mathrm{e}^{-i\theta}}{2i} \qquad \cos\theta = \frac{\mathrm{e}^{i\theta}+\mathrm{e}^{-i\theta}}{2}}$$

Application. Les formules d'Euler permettent notamment de linéariser une expression trigonométrique, c'est-à-dire d'exprimer $\cos^n\theta$ ou $\sin^n\theta$ en fonction de $\cos(p\theta)$ et $\sin(p\theta)$ pour $0\le p\le n$. Ainsi, on a par exemple :

$$\begin{aligned}
\sin^3\theta &= \left(\frac{\mathrm{e}^{i\theta}-\mathrm{e}^{-i\theta}}{2i}\right)^3\\
&= \frac{-1}{8i}\left(\mathrm{e}^{3i\theta}-3\mathrm{e}^{2i\theta}\mathrm{e}^{-i\theta}+3\mathrm{e}^{i\theta}\mathrm{e}^{-2i\theta}-\mathrm{e}^{-3i\theta}\right)\\
&= \frac{-1}{8i}\left(\mathrm{e}^{3i\theta}-3\mathrm{e}^{i\theta}+3\mathrm{e}^{-i\theta}-\mathrm{e}^{-3i\theta}\right)\\
&= \frac{-1}{8i}\left[\underbrace{\mathrm{e}^{3i\theta}-\mathrm{e}^{-3i\theta}}_{2i\sin(3\theta)}-3(\underbrace{\mathrm{e}^{i\theta}-\mathrm{e}^{-i\theta}}_{2i\sin\theta})\right]\\
&= -\frac{\sin(3\theta)}{4}+\frac{3\sin\theta}{4}
\end{aligned}$$

2.3.3 Racines $n^{\text{ièmes}}$ de l'unité

On appelle racine $n^{\text{ième}}$ de l'unité *toute solution de l'équation $z^n = 1$.*
Soit $z = r\mathrm{e}^{i\theta}$ une racine $n^{\text{ième}}$ de l'unité. On a alors nécessairement :

$$
\begin{aligned}
(z^n = 1) &\iff \left(r^n \mathrm{e}^{in\theta} = 1\mathrm{e}^{i0}\right) \\
&\iff \left(\left\{\begin{array}{rcl} r^n &=& 1 \\ n\theta &=& 0 + 2k\pi,\ k \in \mathbb{Z} \end{array}\right.\right) \\
&\iff \left(\left\{\begin{array}{rcl} r &=& 1 \\ n\theta &=& 0 + 2k\pi,\ k \in \mathbb{Z} \end{array}\right.\right) \\
&\iff \left(\left\{\begin{array}{rcl} r &=& 1 \\ \theta &=& \frac{2k\pi}{n},\ k \in \mathbb{Z} \end{array}\right.\right) \\
&\iff \omega_k = 1\ \mathrm{e}^{i\frac{2k\pi}{n}},\ k \in \mathbb{Z}.
\end{aligned}
$$

Les racines $n^{\text{ièmes}}$ de l'unité sont donc :

$$
\omega_0 = 1, \omega_1 = \mathrm{e}^{i\frac{2\pi}{n}}, \omega_2 = \mathrm{e}^{i\frac{4\pi}{n}}, \ldots, \omega_k = \mathrm{e}^{i\frac{2k\pi}{n}}, \ldots, \omega_{n-1} = \mathrm{e}^{i\frac{2(n-1)\pi}{n}}, \underbrace{\mathrm{e}^{i\frac{2n\pi}{n}}}_{\omega_0}, \underbrace{\mathrm{e}^{i\frac{2(n+1)\pi}{n}}}_{\omega_1}, \underbrace{\mathrm{e}^{i\frac{2(n+2)\pi}{n}}}_{\omega_2}, \ldots
$$

On voit ainsi qu'il y n racines $n^{\text{ièmes}}$ de l'unité distinctes, à savoir $\omega_0, \omega_1, \ldots, \omega_{n-1}$. Et comme $\omega_k = \omega_1^k$ pour tout $k \in \{0, 1, \ldots, n-1\}$, on a démontré le résultat suivant :

$$
\boxed{\text{L'équation } z^n = 1 \text{ possède } n \text{ solutions distinctes, } \omega_1^k, \text{ pour } k \in \{0, 1, \ldots, n-1\}, \text{ où } \omega_1 = \mathrm{e}^{i\frac{2\pi}{n}}}
$$

Exemple. L'équation $z^3 = 1$ possède 3 solutions distinctes (les racines $3^{\text{ièmes}}$ de l'unité) qui sont $\omega_0 = 1$, $\omega_1 = \mathrm{e}^{i\frac{2\pi}{3}}$ et $\omega_2 = \mathrm{e}^{i\frac{4\pi}{3}} = -\mathrm{e}^{i\frac{\pi}{3}}$.

Remarque. Pour tout $n \geq 2$, on a

$$
\sum_{k=0}^{n-1} \omega_k = 0.
$$

En effet, comme ω_1 est racine $n^{\text{ième}}$ de l'unité, on a

$$
\begin{aligned}
(\omega_1^n - 1 = 0) &\iff \left(\underbrace{(\omega_1 - 1)}_{\neq 0}\left[\sum_{k=0}^{n-1} \omega_1^k\right] = 0\right) \\
&\iff \left(\sum_{k=0}^{n-1} \underbrace{\omega_1^k}_{\omega_k} = 0\right) \\
&\iff \left(\sum_{k=0}^{n-1} \omega_k = 0\right).
\end{aligned}
$$

2.3.4 Un exemple d'utilisation des nombres complexes en physique

On considère un mouvement sinusoïdal de pulsation ω *:*

$$
v(t) = V\cos(\omega t + \varphi).
$$

En physique, V s'appelle l'amplitude *et φ la* phase*. Toutes les quantités introduites (ω, V et φ) sont réelles. On peut alors écrire*

$$
v(t) = \operatorname{Re}\left(V\mathrm{e}^{i(\omega t + \varphi)}\right) = \operatorname{Re}\left(V\mathrm{e}^{i\varphi}\mathrm{e}^{i\omega t}\right).
$$

L'expression $\mathcal{V} = V\mathrm{e}^{i\varphi}$ s'appelle l'amplitude complexe *du signal v.*
Maintenant, si l'on considère deux signaux

$$
\left\{\begin{array}{rclcl} v_1(t) &=& V_1\cos(\omega t + \varphi_1) &=& \operatorname{Re}\left(V_1\mathrm{e}^{i\varphi_1}\mathrm{e}^{i\omega t}\right) \\ v_2(t) &=& V_2\cos(\omega t + \varphi_2) &=& \operatorname{Re}\left(V_2\mathrm{e}^{i\varphi_2}\mathrm{e}^{i\omega t}\right), \end{array}\right.
$$

de même pulsation ω, leur somme s est :

$$s(t) = \mathrm{Re}\left((V_1 \mathrm{e}^{i\varphi_1} + V_2 \mathrm{e}^{i\varphi_2})\mathrm{e}^{i\omega t}\right).$$

Il s'agit donc à nouveau d'un signal sinusoïdal de pulsation ω, dont l'amplitude complexe est la somme des deux amplitudes complexes de chacun des signaux v_1 et v_2.
Dans le cas particulier où $V_1 = V_2 = V$, on a de plus :

$$V_1 \mathrm{e}^{i\varphi_1} + V_2 \mathrm{e}^{i\varphi_2} = V \mathrm{e}^{i\frac{\varphi_1+\varphi_2}{2}} (\underbrace{\mathrm{e}^{i\frac{\varphi_1-\varphi_2}{2}} + \mathrm{e}^{i\frac{-\varphi_1+\varphi_2}{2}}}_{2\cos\left(\frac{\varphi_1-\varphi_2}{2}\right)}) = 2V\cos\left(\frac{\varphi_1-\varphi_2}{2}\right)\mathrm{e}^{i\frac{\varphi_1+\varphi_2}{2}},$$

ce qui permet d'établir avec très peu de calculs que :

- *l'amplitude de s est $2V\cos\left(\frac{\varphi_1-\varphi_2}{2}\right)$*
- *la phase de s est $\frac{\varphi_1+\varphi_2}{2}$.*

3 Polynômes

Dans tout ce chapitre, K désigne soit $\mathbb{R}$, soit $\mathbb{C}$.

On considère ici des polynômes à coefficients dans K de la variable $x \in K$:

$$P(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_p x^p, \; a_k \in K \text{ pour } 0 \leq k \leq p.$$

Si $a_p \neq 0$, p est le degré du polynôme P, noté $\deg P$. Un polynôme à coefficients dans K est donc une suite de termes appartenant à K, qui sont tous nuls à partir d'un certain rang :

$$P = (a_0, a_1, a_2, \ldots, a_p, 0, 0, \ldots),$$

ce que l'on note plus économiquement $P = (a_k)_{k\in\mathbb{N}}$ en gardant à l'esprit que $a_k = 0$ pour tout $k \geq p+1$.

On note $K[X]$, l'ensemble des polyômes à coefficients dans K de la variable $x \in K$.

3.1 Opérations sur les polynômes

Soient deux polynômes $P = (a_i)_{i\in\mathbb{N}}$ et $Q = (b_j)_{j\in\mathbb{N}}$.

3.1.1 Addition et produit par un nombre appartenant à K

Par définition, le polynôme somme est $P + Q = (c_k)_{k\in\mathbb{N}}$ avec $c_k = a_k + b_k$ pour tout $k \in \mathbb{N}$.

Conséquence. Notons $p = \deg P$ et $q = \deg Q$, de sorte que $P = (a_0, a_1, a_2, \ldots, a_p, 0, 0, \ldots)$ avec $a_p \neq 0$ et $Q = (b_0, b_1, b_2, \ldots, b_q, 0, 0, \ldots)$ avec $b_q \neq 0$. On voit facilement que :
- *si $p \neq q$, $\deg(P+Q) = \max(\deg P, \deg Q)$*
- *si $p = q$, $\deg(P+Q) \leq p$.*

Ceci implique :

$$\boxed{\deg(P+Q) \leq \max(\deg P, \deg Q)}$$

Remarque : cas du polynôme nul. Dans l'inégalité précédente on a supposé que $p \geq 0$ et $q \geq 0$, c'est-à-dire que P et Q sont différents du polynôme nul (polynôme dont tous les coefficients sont nuls), noté $\underline{0}$. Néanmoins, en posant $\deg \underline{0} = -\infty$ et en convenant que $-\infty \leq k$ et $-\infty \pm k = -\infty$ pour tout $k \in \mathbb{N}$, l' inégalité précédente reste valable lorsque l'un des polynômes P ou Q est égal à $\underline{0}$.

Ensuite, pour tout $\lambda \in K$, on définit le polynôme λP en posant : $\lambda P = (\lambda a_i)_{i\in\mathbb{N}}$.
Remarque. L'égalité entre les polynômes P et Q se définit :
- *en tant que suites de termes appartenant à K par l'égalité des coefficients :*

$$(P = Q) \iff (a_0 = b_0, a_1 = b_1, \ldots, a_p = b_p)$$

- *en tant que fonctions par : $(P = Q) \iff (P(x) = Q(x), \; \forall x \in K)$.*

On admet que ces deux points de vue sont équivalents.

3.1.2 Produit de deux polynômes

Par définition, le polynôme produit de P par Q est

$$PQ = (c_k)_{k\in\mathbb{N}}, \text{ avec } c_k = \sum_{i=0}^{k} a_i b_{k-i} \text{ pour tout } k \in \mathbb{N},$$

c'est-à-dire

$$c_0 = a_0 b_0, c_1 = a_0 b_1 + a_1 b_0, c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0, \ldots, c_{p+q} = a_p b_q \tag{3}$$

Comme $a_p \neq 0$ et $b_q \neq 0$, on a donc $c_{p+q} \neq 0$. Par ailleurs il est clair que $c_n = 0$ dès que $n > p + q$, ce qui prouve :

$$\boxed{\deg(PQ) = \deg P + \deg Q}$$

On vérifie alors à l'aide de cette égalité que :

$$(PQ = \underline{0}) \Longleftrightarrow (P = \underline{0} \text{ ou } Q = \underline{0})\,.$$

Il résulte facilement de la définition (3) des coefficients du polynôme PQ que la multiplication polynomiale est commutative : $PQ = QP$.

Remarque. Pour chaque $k \in \mathbb{N}$, posons

$$E_k = (\delta_{jk})_{j\in\mathbb{N}} \text{ où } \delta_{jk} = \begin{cases} 1 & \text{si } j = k \\ 0 & \text{sinon,} \end{cases}$$

c'est-à-dire :

$$E_0 = (1, 0, 0, \ldots),\ E_1 = (0, 1, 0, 0, \ldots),\ E_2 = (0, 0, 1, 0, 0, \ldots),\ \text{etc...}$$

Compte tenu de la définition du produit de deux polynômes, on peut écrire :

$$E_p = E_1^p \text{ pour tout } p \in \mathbb{N}.$$

Ainsi, comme tout polynôme $P = (a_0, a_1, \ldots, a_p, 0, 0, \ldots)$ s'écrit également

$$P = a_0E_0 + a_1E_1 + a_2E_2 + \ldots + a_pE_p,$$

on obtient, en posant préalablement $X = E_1$ (ce symbole X s'appelle l'indéterminée) que $P = a_0X^0 + a_1X^1 + a_2X^2 + \ldots + a_pX^p$, ce que l'on note usuellement :

$$P = a_0 + a_1X + a_2X^2 + \ldots + a_pX^p.$$

La fonction de K à valeurs dans K, $x \mapsto \tilde{P}(x) = a_0 + a_1x + a_2x^2 + \ldots + a_px^p$ (obtenue en remplaçant l'indéterminée X -qui est en fait un polynôme- par l'élement x de K dans l'expression de P) s'appelle la fonction polynôme associée à P. Vu la remarque finale de §3.1.1 il n'y a pas lieu de faire la distinction entre le polynôme P et sa fonction polynôme associée $\tilde{P}$, que l'on notera également P désormais.

3.2 Division des polynômes

3.2.1 Division euclidienne

Etant donnés deux polynômes A et B avec $B \neq 0$, on démontre (on l'admet dans ce cours) qu'il existe un unique couple de polynômes (Q, R) tel que les deux conditions suivantes soient satisfaites simultanément :

$$\begin{cases} (i) & A = BQ + R \\ (ii) & \deg R < \deg B. \end{cases}$$

Les polynômes B, Q et R s'appellent respectivement le diviseur, le quotient et le reste de la division euclidienne de A par B. Le résultat précédent est généralement appelé théorème de division euclidienne.

Exemple. Le quotient de la division euclidienne de $X^3 - 2X^2 + 1$ par $X^2 - X + 2$ est $X - 1$ et le reste est $-3X + 3$.

On dit que B divise A ou que B est un diviseur de A ou bien encore que A est divisible par B, si le reste R de la division euclidienne de A par B est le polynôme nul : $R = \underline{0}$.

Le cas particulier de la division par $X - a$, $a \in K$. *L'égalité de division euclidienne de P par $X - a$ s'écrit*

$$P = (X - a)Q + R \text{ avec } \deg R < 1. \tag{4}$$

Par suite, $\deg R \leq 0$ donc R est un polynôme constant (éventuellement nul). Comme l'égalité (4) est valable pour tout $x \in K$, elle est vraie en particulier si $x = a$, ce qui implique $R = P(a)$. Par suite :

$$\boxed{(P \text{ est divisible par } X - a) \Longleftrightarrow (P(a) = 0)} \tag{5}$$

Ce résultat se généralise au cas de plusieurs racines distinctes. Ainsi pour $a \neq b$, on a :

$$(P \text{ est divisible par } (X - a)(X - b)) \Longleftrightarrow (P(a) = P(b) = 0)\,. \tag{6}$$

3.2.2 Division selon les puissances croissantes

Si A et B sont deux polynômes tels que $B(0) \neq 0$, on admettra qu'il existe un unique couple (Q, R) de polynômes tels que

$$\begin{cases} (i) & A = BQ + X^{n+1}R \\ (ii) & \deg Q \leq n. \end{cases}$$

Les polynômes Q et R s'appellent respectivement le $quotient$ et le $reste$ de la $division\ suivant\ les\ puissances\ croissantes\ de\ A\ par\ B\ à\ l'ordre\ n$.

Dans la pratique, les polynômes Q et R sont obtenus en ordonnant A et B en puissances croissantes et en procédant par divisions successives jusqu'à ce que l'on puisse mettre X^{n+1} en facteur dans le reste. Il est donc nécessaire de préciser à quel ordre la division doit être effectuée.

Exemple. La division à l'ordre 2 de $A = 1 + X - 3X^3$ par $B = 1 + X^2$ s'écrit :

$$A = B(1 + X - X^2) + X^3(-X - 3).$$

3.3 Zéro d'un polynôme

3.3.1 Formule de Taylor

Soit $a \in \mathbb{R}$. Pour tout polynôme $P = a_0 + a_1X + a_2X^2 + \ldots + a_pX^p \in \mathbb{R}_p[X]$, il existe un unique $(p+1)$-uplet $(\alpha_0, \alpha_1, \ldots, \alpha_p)$ de réels tel que

$$\forall x \in \mathbb{R},\ P(x) = \alpha_0 + \alpha_1(x-a) + \alpha_2(x-a)^2 + \ldots + \alpha_p(x-a)^p.$$

En effet, par dérivations successives, il vient

$$\begin{cases} P'(x) & = & \alpha_1 + 2\alpha_2(x-a) + 3\alpha_3(x-a)^2 \ldots + p\alpha_p(x-a)^{p-1} \\ P''(x) & = & 2\alpha_2 + 6\alpha_3(x-a) + \ldots + p(p-1)\alpha_p(x-a)^{p-2} \\ \vdots & \vdots & \vdots \\ P^{(p)}(x) & = & p(p-1)(p-2)\ldots[p-(p-1)]\alpha_p(x-a)^{p-p} = p!\alpha_p, \end{cases}$$

ce qui implique immédiatement :

$$\alpha_0 = P(a),\ \alpha_1 = P'(a),\ \alpha_2 = \frac{P''(a)}{2!}, \ldots, \alpha_p = \frac{P^{(p)}(a)}{p!}.$$

D'où la $formule\ de\ Taylor$:

$$\boxed{P(x) = P(a) + P'(a)(x-a) + \tfrac{P''(a)}{2!}(x-a)^2 + \ldots + \tfrac{P^{(p)}(a)}{p!}(x-a)^p,\ \forall\ x \in \mathbb{R}}$$

Exemple. La formule de Taylor du polynôme $P = X^2 + X + 1$ en $a = 1$ s'écrit :

$$P(x) = 3 + 3(x-1) + (x-1)^2.$$

3.3.2 Racine et multiplicité

Soit P un polynôme à coefficients dans K.
On dit que a est $racine\ (ou\ zéro)\ de\ P$ si P s'annule au point a : $P(a) = 0$. D'après l'équivalence (5), on peut donc dire que a est racine de P si $X - a$ divise P, c'est-à-dire s'il existe un polynôme Q tel que $P = (X-a)Q$.
On peut ensuite se poser la question de savoir si a est racine du polynôme Q. Si tel est le cas, $X - a$ divise Q, donc il existe un polynôme R tel que $Q = (X-a)R$, ce qui entraîne finalement $P = (X-a)^2\ R$.
Ainsi, lorsque l'on est en présence d'un zéro, a, de P, il est naturel d'essayer de connaître la "plus grande puissance de $X - a$" qui divise P. Compte tenu de cette remarque, on dira que $a\ est\ racine\ (ou\ zéro)\ de\ multiplicité\ m$ $(m \geq 1)$ du polynôme P, si l'on peut mettre P sous la forme

$$P = (X-a)^m Q \text{ avec } Q(a) \neq 0.$$

L'entier $m \geq 1$ s'appelle $l'ordre\ de\ multiplicité$ (ou plus simplement $la\ multiplicité$ ou encore $l'ordre$) de a en tant que zéro de P. La condition $Q(a) \neq 0$ signifiant en vertu de (5) que Q n'est pas divisible par $X - a$, on a donc immédiatement l'équivalence suivante :

$$(a \text{ est racine de } P \text{ de multiplicité } m) \Longleftrightarrow \left(\begin{cases} (i) & (X-a)^m \text{ divise } P \\ (ii) & (X-a)^{m+1} \text{ ne divise pas } P. \end{cases} \right)$$

Quoiqu'il en soit, le degré du polynôme P étant toujours noté p, la formule de Taylor permet d'écrire

$$\begin{aligned} P(x) &= P(a) + P'(a)(x-a) + \frac{P''(a)}{2!}(x-a)^2 + \ldots + \frac{P^{(m-1)}(a)}{(m-1)!}(x-a)^{m-1} \\ &+ (x-a)^m \left[\frac{P^{(m)}(a)}{m!} + \frac{P^{(m+1)}(a)}{(m+1)!}(x-a) + \ldots + \frac{P^{(p)}(a)}{p!}(x-a)^{p-m} \right], \end{aligned}$$

on a donc l'équivalence

$$\begin{aligned} &\left(\begin{cases} (i) & P(x) = (x-a)^m Q(x) \\ (ii) & Q(a) \neq 0 \end{cases} \right) \\ \Longleftrightarrow \\ &\left(\begin{cases} (i') & \forall x \in K,\ P(a) + P'(a)(x-a) + \frac{P''(a)}{2!}(x-a)^2 + \ldots + \frac{P^{(m-1)}(a)}{(m-1)!}(x-a)^{m-1} = 0 \\ (ii') & \frac{P^{(m)}}{m!}(a) \neq 0, \end{cases} \right), \end{aligned}$$

ce qui entraîne finalement :

$$\boxed{(a \text{ est racine de } P \text{ de multiplicité } m) \Longleftrightarrow \left(\begin{cases} (i) & P(a) = P'(a) = \ldots = P^{(m-1)}(a) = 0 \\ (ii) & P^{(m)}(a) \neq 0. \end{cases} \right)} \quad (7)$$

3.4 Factorisation des polynômes

3.4.1 Factorisation dans $\mathbb{C}[X]$

Elle repose essentiellement sur le résultat (admis) suivant :

Théorème 3.1. *(Théorème de d'Alembert). Tout polynôme de degré p non nul possède exactement p zéros (distincts ou confondus) dans $\mathbb{C}$.*

Lorsque certains de ces zéros sont confondus, on a seulement $n < p$ zéros distincts $z_1, z_2, \ldots, z_n$. En notant m_i la multiplicité de z_i en tant que zéro de $P = a_0 + a_1X + \ldots + a_pX^p$ pour tout i de 1 à n, on a alors :

$$m_1 + m_2 + \ldots + m_n = p.$$

L'équivalence (6) permet alors d'écrire :

$$\boxed{P = a_p(X-z_1)^{m_1}(X-z_2)^{m_2} \ldots (X-z_n)^{m_n}}$$

Lorsque P est écrit sous cette forme, on dit qu'il est $décomposé\ en\ produit\ de\ facteurs\ irréductibles\ dans$ $\mathbb{C}[X]$, ou plus simplement $factorisé\ dans$ $\mathbb{C}[X]$. Comme tous les polynômes de cette factorisation sont de degrés au plus 1, on dit que P est $scindé$ dans $\mathbb{C}$.

3.4.2 Factorisation dans $\mathbb{R}[X]$

Supposons maintenant que $P = a_0 + a_1X + \ldots + a_pX^p$ est un polynôme à coefficients réels. C'est donc a $fortiori$ un polynôme à coefficients complexes, que l'on peut le décomposer en produit de facteurs irréductibles dans $\mathbb{C}$, comme on vient de le voir au §3.4.1 :

$$P = a_p(X-z_1)^{m_1}(X-z_2)^{m_2} \ldots (X-z_n)^{m_n}.$$

Mais, même si P est à coefficients réels, certains zéros de P sont éventuellement complexes non réels. Quitte à réindexer la liste $z_1, z_2, \ldots, z_n$, on peut supposer qu'il existe un entier $k \leq n$ tel que que $z_1, z_2, \ldots, z_k$ sont

réels et $z_{k+1}, z_{k+2}, \ldots, z_n$ sont complexes non réels. Afin d'améliorer les notations, on notera désormais x_i plutôt que z_i, $1 \leq i \leq k$, les zéros réels de P.
Maintenant, si z est un zéro complexe non réel de $P = a_0 + a_1 X + \ldots + a_p X^p$, on a

$$P(z) = a_0 + a_1 z + \ldots + a_p z^p = 0,$$

et, le conjugué $\overline{P(z)}$ de $P(z)$, qui est également nul, s'écrit :

$$\begin{aligned}
\overline{P(z)} &= \overline{a_0 + a_1 z + \ldots + a_p z^p} \\
&= \overline{a_0} + \overline{a_1}\,\overline{z} + \ldots + \overline{a_p}\,\overline{z^p} \\
&= a_0 + a_1 \overline{z} + \ldots + a_p \overline{z}^p \\
&= P(\overline{z}),
\end{aligned}$$

car tous les coefficients a_i, $0 \leq i \leq p$, sont réels. Ceci montre que $\overline{z}$ est donc également zéro de P. On peut même montrer que si z est zéro complexe non réel de P de multiplicité m, alors la multiplicité de $\overline{z}$ en tant que zéro (complexe non réel) de P est également m. Ainsi, la liste $z_{k+1}, z_{k+2}, \ldots, z_n$ des zéros complexes non réels de P se met également sous la forme

$$\{z_{k+1}, z_{k+2}, \ldots, z_n\} = \{\alpha_1, \overline{\alpha_1}, \alpha_2, \overline{\alpha_2}, \ldots, \alpha_d, \overline{\alpha_d}\},$$

avec évidemment $2d = n - k$. Pour tout j de 1 à d, chacun des α_j et $\overline{\alpha_j}$ est donc un zéro complexe non réel de P de même multiplicité β_j. Avec ces nouvelles notations, la factorisation de P dans $\mathbb{C}$ devient alors :

$$P = a_p(X-x_1)^{m_1}(X-x_2)^{m_2}\ldots(X-x_k)^{m_k}[(X-\alpha_1)(X-\overline{\alpha_1})]^{\beta_1}[(X-\alpha_2)(X-\overline{\alpha_2})]^{\beta_2}\ldots[(X-\alpha_d)(X-\overline{\alpha_d})]^{\beta_d}.$$

Maintenant, si l'on convient de poser $\alpha_r = u_r + iv_r$ pour tout r de 1 à d, l'égalité

$$(X - \alpha_r)(X - \overline{\alpha_r}) = (X - u_r)^2 + v_r^2,$$

donne :

$$\boxed{P = a_p(X - x_1)^{m_1}(X - x_2)^{m_2}\ldots(X - x_k)^{m_k}[(X - u_1)^2 + v_1^2]^{\beta_1}[(X - u_2)^2 + v_2^2]^{\beta_2}\ldots[(X - u_d)^2 + v_d^2]^{\beta_d}}$$

Cette fois, P est écrit comme produit de polynômes de $\mathbb{R}[X]$. On dit alors qu'il est décomposé en produit de facteurs irréductibles dans $\mathbb{R}[X]$ ou plus simplement factorisé dans $\mathbb{R}[X]$.